

CLAIMS

What is claimed is:

1 1. A method of comparing access control lists to configure a security policy on a
2 network, the method comprising the computer-implemented steps of:
3 identifying one or more first sub-entries in a first access control list;
4 identifying one or more second sub-entries in a second access control list;
5 programmatically determining whether a first access control list is functionally
6 equivalent to a second access control list in order to configure the security
7 policy on the network by determining whether each first sub-entry is
8 equivalent to one or more of the second sub-entries; and
9 determining that the first access control is functionally equivalent to the second access
10 control list only when each of the first sub-entries is equivalent to one or more
11 of the second sub-entries.

1 2. A method as recited in Claim 1, wherein programmatically determining whether a
2 first access control list is equivalent to a second access control list includes:
3 identifying a dimensional range for each policy action specified in the first access
4 control list, the dimensional range of each policy action characterizing
5 communication packets specified by one or more entries in the first access
6 control list for that that policy action;
7 identifying a dimensional range for each policy action specified in the second access
8 control list, the dimensional range of each policy action characterizing
9 communication packets specified by one or more entries in the second access
10 control list for that that policy action; and
11 determining whether the dimensional range identified for each policy action in the
12 first access control list is equivalent to the dimensional range identified for
13 each policy action in the second access control list.

3. A method as recited in Claim 2, wherein identifying a dimensional range for each policy action specified in the first access control list and in the second access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list and in the second access control list.

4. A method as recited in Claim 2, wherein identifying a dimensional range for each policy action specified in the first access control list and in the second access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list.

5. A method as recited in Claim 2, wherein identifying a dimensional range for each policy action specified in the first access control list and in the second access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list.

6. A method as recited in Claim 1, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list includes:
determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the second access control list that specify the policy action of the entry in the first access control list.

1 7. A method as recited in Claim 1, wherein the first access control list and the second
2 access control list each specify a plurality of entries, and each entry identifies a dimensional
3 range for a policy action, the dimensional range characterizing communication packets that
4 are to be affected by the policy action, and wherein programmatically determining whether a
5 first access control list is equivalent to the second access control list includes:

6 determining whether each entry in the first access control list has a dimensional range
7 that is either equivalent to or contained by the dimensional range of one or
8 more entries in the second access control list that specify the policy action of
9 the entry in the first access control list; and

10 determining whether each entry in the second access control list has a dimensional
11 range that is either equivalent to or contained by the dimensional range of one
12 or more entries in the first access control list that specify the same policy
13 action.

1 8. A method as recited in Claim 1, wherein programmatically determining whether a
2 first access control list is equivalent to a second access control list includes determining
3 whether the first access control list having one hundred or more entries is equivalent to the
4 second access control list having one hundred or more entries.

1 9. A method of comparing access control lists to configure a security policy on a
2 network, the method comprising:
3 identifying a dimensional range and a policy action for each entry in a first access
4 control;
5 identifying all overlapping dimensional ranges in the first access control list, each
6 overlapping dimensional range corresponding to where the dimensional ranges
7 of two or more entries in the first access control list overlap;
8 identifying all non-overlapping dimensional ranges in the first access control list, each
9 of the non-overlapping dimensional ranges corresponding to dimensional
10 ranges of entries in the first access control list that do not overlap dimensional
11 ranges of other entries in the first access control list;

12 identifying a policy action for each identified overlapping dimensional range of the
 13 first access control list;
 14 identifying a policy action for each identified non-overlapping dimensional range of
 15 the first access control list; and
 16 determining whether each identified overlapping and non-overlapping dimensional
 17 range identified from the first access control list is contained by or equal to a
 18 dimensional range of one or more entries in a second access control list in
 19 which the one or more entries of the second access control list have the policy
 20 action of that identified overlapping or non-overlapping dimensional range.

1 10. A method as recited in Claim 9, further comprising:
 2 identifying a dimensional range and a policy action for each entry in the second
 3 access control;
 4 identifying all overlapping dimensional ranges in the second access control list, each
 5 overlapping dimensional range corresponding to where the dimensional ranges
 6 of two or more entries in the second access control list overlap;
 7 identifying all non-overlapping dimensional ranges in the second access control list,
 8 each of the non-overlapping dimensional ranges corresponding to dimensional
 9 ranges of entries in the second access control list that do not overlap
 10 dimensional ranges of other entries in the second access control list;
 11 identifying a policy action for each identified overlapping dimensional range in the
 12 second access control list;
 13 identifying a policy action for each identified non-overlapping dimensional range of
 14 the second access control list; and
 15 determining whether each identified overlapping and non-overlapping dimensional
 16 range identified from the second access control list is contained by or equal to
 17 a dimensional range of one or more entries in the first access control list in
 18 which the one or more entries of the first access control list have the policy
 19 action of that identified overlapping or non-overlapping dimensional range.

11. A method as recited in Claim 9, wherein:

identifying a dimensional range and a policy action for each entry in the second access control list;

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of two or more entries in the second access control list overlap;

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

identifying a policy action for each identified overlapping dimensional range of the second access control list;

identifying a policy action for each identified non-overlapping dimensional range of the second access control list; and

and wherein determining whether each identified overlapping and non-overlapping dimensional range of the first access control list is contained by or equal to a dimensional range of one or more entries in a second access control list includes determining whether each identified overlapping and non-overlapping dimensional range identified from the first access control list is contained by or equal to one or more overlapping and non-overlapping dimensional ranges of the second access control list.

12. A method as recited in Claim 9, wherein identifying a policy action for each identified overlapping dimensional range of the first access control list includes using a conflict rule to determine the policy action from a first policy action of a first entry having a dimensional range within the overlapping dimensional range, and from a second policy action of a second entry having a dimensional range within the overlapping dimensional range, wherein the second policy conflicts with the first policy.

1 13. A method as recited in Claim 12, wherein using a conflict rule to determine the policy
2 action selecting one of the first policy or the second policy based on the selected first or
3 second policy being newer.

1 14. A method as recited in Claim 9, wherein identifying a dimensional range and a policy
2 action for each entry in the first access control list includes identifying a source address range
3 and a destination address range for communication packets specified by each of the entries in
4 the first access control list.

1 15. A method as recited in Claim 9, wherein identifying a dimensional range and a policy
2 action for each entry in the first access control list includes identifying a source port range
3 and a destination port range for communication packets specified by each of the entries in the
4 first access control list.

1 16. A method as recited in Claim 9, wherein identifying a dimensional range and a policy
2 action for each entry in the first access control list includes identifying a communication
3 protocol for communication packets specified by each of the entries in the first access control
4 list.

1 17. A computer readable medium for comparing access control lists to configure a
2 security policy on a network, the computer readable medium carrying instructions for
3 performing the steps of:
4 identifying one or more first sub-entries in a first access control list;
5 identifying one or more second sub-entries in a second access control list;
6 programmatically determining whether a first access control list is functionally
7 equivalent to a second access control list in order to configure the security
8 policy on the network by determining whether each first sub-entry is
9 equivalent to one or more of the second sub-entries; and

10 determining that the first access control is functionally equivalent to the second access
 11 control list only when each of the first sub-entries is equivalent to one or more of the
 12 second sub-entries.

1 18. A computer readable medium as recited in Claim 17, wherein instructions for
 2 programmatically determining whether a first access control list is equivalent to a second
 3 access control list include instructions for:
 4 identifying a dimensional range for each policy action specified in the first access
 5 control list, the dimensional range of each policy action characterizing
 6 communication packets specified by one or more entries in the first access
 7 control list for that that policy action;
 8 identifying a dimensional range for each policy action specified in the second access
 9 control list, the dimensional range of each policy action characterizing
 10 communication packets specified by one or more entries in the second access
 11 control list for that that policy action; and
 12 determining whether the dimensional range identified for each policy action in the
 13 first access control list is equivalent to the dimensional range identified for
 14 each policy action in the second access control list.

1 19. A computer readable medium as recited in Claim 17, wherein instructions for
 2 identifying a dimensional range for each policy action specified in the first access control list
 3 and in the second access control list include instructions for identifying a source address
 4 range and a destination address range for communication packets specified by each of the
 5 entries in the first access control list and in the second access control list.

1 20. A computer readable medium as recited in Claim 19, wherein instructions for
 2 identifying a dimensional range for each policy action specified in the first access control list
 3 and in the second access control list include instructions for identifying a source port range
 4 and a destination port range for communication packets specified by each of the entries in the
 5 first access control list and in the second access control list.

21. A computer-readable medium as recited in Claim 17, wherein instructions for identifying a dimensional range for each policy action specified in the first access control list and in the second access control list include instructions for identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list.

22. A computer-readable medium as recited in Claim 17, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein instructions for programmatically determining whether a first access control list is equivalent to the second access control list includes instructions for determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the second access control list that specify the same policy action.

23. A computer-readable medium as recited in Claim 17, wherein the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein instructions for programmatically determining whether a first access control list is equivalent to the second access control list includes instructions for:

- determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the second access control list that specify the same policy

- action; and

- determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the first access control list that specify the same policy action.

1 24. The computer-readable medium of Claim 17, wherein the first access control list and
2 the second access control list each include one hundred or more entries.

1 25. A computer system for comparing access control lists to configure a security policy
2 on a network, the computer system comprising:
3 means for identifying one or more first sub-entries in a first access control list;
4 means for identifying one or more second sub-entries in a second access control list;
5 means for programmatically determining whether a first access control list is
6 functionally equivalent to a second access control list in order to configure the
7 security policy on the network by determining whether each first sub-entry is
8 equivalent to one or more of the second sub-entries; and
9 means for determining that the first access control is functionally equivalent to the
10 second access control list only when each of the first sub-entries is
11 equivalent to one or more of the second sub-entries.

1 26. A policy server communicatively coupled to one or more security devices in a
2 network to configure a security policy on a network, the policy server comprising:
3 a processor;
4 a network interface that communicatively couples the processor to the network to
5 receive one or more flows of packets therefrom;
6 a memory; and
7 one or more sequences of instructions in the memory which, when executed by the
8 processor, cause the processor to carry out the steps of:
9 identifying one or more first sub-entries in a first access control list;
10 identifying one or more second sub-entries in a second access control list;
11 programmatically determining whether a first access control list is functionally
12 equivalent to a second access control list in order to configure the security
13 policy on the network by determining whether each first sub-entry is
14 equivalent to one or more of the second sub-entries; and

15 determining that the first access control is functionally equivalent to the second access
16 control list only when each of the first sub-entries is equivalent to one or more
17 of the second sub-entries.

1 27. The policy server of claim 26, wherein further comprising a memory to store a
2 plurality of access control lists, including the first access control list and the second access
3 control list, and wherein the processor is configured to configure each security device on the
4 network with at least one of the plurality of access control lists.

1 28. The policy server of claim 26, wherein the processor is configured to:
2 identify a dimensional range for each policy action specified in the first access control
3 list, the dimensional range of each policy action characterizing communication
4 packets specified by one or more entries in the first access control list for that
5 that policy action;
6 identify a dimensional range for each policy action specified in the second access
7 control list, the dimensional range of each policy action characterizing
8 communication packets specified by one or more entries in the second access
9 control list for that that policy action; and
10 determine whether the dimensional range identified for each policy action in the first
11 access control list is equivalent to the dimensional range identified for each
12 policy action in the second access control list.